CAE Tech Talk

17 March 2022

An Empirical Investigation of Static and Polymorphic Tactile Stimuli's Effect on Habituation to Cybersecurity Warnings
(1:00 – 1:50 pm EST)

Fast-Flux Attack Detection using Machine Learning and Genetic Algorithms

(2:00 – 2:50 pm EST)

Mark your calendars and come join your friends in the CAE community for a Tech Talk. CAE Tech Talks are free and conducted live in real-time over the Internet so no travel is required. Capitol Technology University (CTU) hosts the presentations using Zoom which employs slides, VOIP, and chat for live interaction. Just log in as "Guest" and enjoy the presentation(s).

Below is a description of the presentations and logistics of attendance:

PRESENTATION #1

Topic: An Empirical Investigation of Static and Polymorphic Tactile Stimuli's Effect on Habituation to Cybersecurity Warnings

Time: 1:00pm – 1:50 pm EST

Location: https://captechu.zoom.us/j/664120328

Just log in as "Guest" and enter your name. No password required.

Presenter(s):

Javier Coto, Ph.D. Candidate in Cybersecurity Management, Nova Southeastern University

Yair Levy, Ph.D, Nova Southeastern University

Description: Today social engineering is being consistently presented as the greatest cybersecurity vulnerability. Users' habituation to cybersecurity warnings is a large factor contributing to this phenomenon. According to prior literature, traditional cryptography-based security framework is mainly ineffective in counterbracing the effects of habituation. Furthermore, this problem has been compounded by the volume of non-essential notifications, sometimes very similar in look and feel to the critical cybersecurity warnings, which causes a generalization of habituation to cybersecurity warnings. This generalization increases the vulnerabilities of any cybersecurity plan by potentially habituating users to cybersecurity warning never seen before. The main goal of this presentation is to discuss an on-going research study we are conducting to mitigate this cybersecurity attack vector through increase of sensitization. Sensitization being an energizing process that strengthens attention and counterbalances habituation, in our study it is done through a vibrating mouse. This study will triangulate across measures using an Electroencephalogram (EEG) machine (Emotiv Epoc Flex 32 channels) and mouse cursor indicators (area under the curve, initial acceleration, and average speeds) to increase its validity of assessing users' habituation to cybersecurity warnings. The presentation will outline the rational for the study and discuss the research design developed to conduct the experiments with 50 participants. Additionally, discussion will outline the anticipated comparison between static flutter-vibration and polymorphic flutter-vibration assessments. Finally, we will discuss the assessment for any statistically significant mean differences of repetition suppression (habituation) when controlled for demographics such as working memory capacity, number of speaking languages, job type, daily Internet usage, and dominant hand orientation.

PRESENTATION #2

Topic: Fast-Flux Attack Detection using Machine Learning and Genetic Algorithms

Time: 2:00pm – 2:50 pm EST

Location: https://captechu.zoom.us/j/664120328

Just log in as "Guest" and enter your name. No password required.

Presenter(s): Ahmet Aksoy, Ph.D, University of Central Missouri

Description: In our work, we present an entirely automated fast-flux detection approach using machine learning and genetic algorithms without expert input. Such an automated approach helps detect the uniqueness in malicious hosts' behavior from their network traffic even when their behavior changes. The presented approach makes fast-flux detection insusceptible to changes in infected hosts as long as a representative dataset is provided, making it more difficult for attackers to hide their hosts

CAE Tech Talks are recorded; view them here: https://www.caecommunity.org/resources/cae-tech-talk-resources

For questions on CAE Tech Talk, please send email to CAETechTalk@nsa.gov